

~~SECRET~~**ROUTING AND RECORD SHEET**

SUBJECT: (Optional) Proposed Secure Video Teleconferencing System (SVTS)
 Concept of Operations [redacted]

FROM: [redacted]
 Director of Security [redacted]

EXTENSION

NO.

OS 8-5680

DATE

13 DEC 1988

TO: (Officer designation, room number, and building)

DATE

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. Executive Secretary
 7E12 HDQS

RECEIVED

FORWARDED

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14. Regrade Unclassified When
 Separated from Secret Attachment

15.

FORM 1-79 **610** USE PREVIOUS EDITIONS

~~SECRET~~

DCI
 EXEC
 REG

L-108-IR

NSDD-95

S E C R E T

13 DEC 1988

MEMORANDUM FOR: Executive Secretary

FROM:

Director of Security

SUBJECT: Proposed Secure Video Teleconferencing System
(SVTS) Concept of Operations

REFERENCE: Memo fm NSA dtd 25 Oct 88, Same Subj,
ER 88-4040X

1. I have reviewed the draft of the Secure Video
Teleconferencing System (SVTS) Concept of Operations put forth
by the Operations Center Subgroup of the Crisis Management
Working Group and find that our concerns regarding these
systems have been addressed.

2. If there are any additional questions contact
Chief, Policy Branch, Policy and Plans
Staff/OS on secure extension

S E C R E T

Page Denied

Next 1 Page(s) In Document Denied

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Proposed Secure Video Teleconferencing System
(SVTS) Concept of Operations

FROM:

Chief, CIA Operations Center
Room 7F27 HQS

EXTENSION

NO.

ER 88-4040/1

DATE

4 November 1988

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1.
D/CPAS
7F16 HQS

4 Nov 88 JSL

2.
DDI Registry
7E47 HQS3.
DDI
7E44 HQS4.
Executive Registry
7F12 HQS

07 NOV 1988

5.
Executive Secretary
7E13 HQS

11 JB

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

✓ L-108-IR - NSDP 95
CR C-204-IR

SECRET

4 November 1988

NOTE FOR: DDI

STAT

FROM:

Chief, CIA Operations Center

SUBJECT: Proposed Secure Video
Teleconferencing System (SVTS)
Concept of Operations

As a member of both the Crisis Management Working Group (CMWG) and the Operations Center Sub-Group, we participated in the preparation of the concept of operations for the Secure Video Teleconferencing System (SVTS). It is the Community's first formal document establishing authorities, responsibilities, and procedures for SVTS. My reply was coordinated with the NIO/Warning, a member of the CMWG.

STAT

25X1

25X1

Central Intelligence Agency



Washington, D.C. 20505

7 November 1988

25X1
MEMORANDUM FOR:

[Redacted]
Executive Secretary
National Security Council

25X1
SUBJECT: Proposed Secure Video Teleconferencing System
(SVTS) Concept of Operations [Redacted]

REFERENCE: Your Memo dtd. 25 October 1988, Same Subject

25X1
1. CIA generally agrees with the draft SVTS Concept of Operations, dated 20 October 1988. [Redacted]

25X1
2. We are particularly pleased with the rewrite of paragraph 5b on page 5, which now clearly and correctly defines the system as a telecommunications tool and which as stated provides for maximum user convenience and operational effectiveness. We expect, however, that as external porting becomes more prevalent, the CMWG will be asked to review this issue. [Redacted]

25X1
25X1
3. As concerns paragraph 3f. We agree that each node should maintain a comprehensive log of its conferences, but believe the SVTS project office, as a result of the Hub scheduling activities covered in paragraph 3d, will be able to provide a consolidated record of use. Moreover, we do not believe providing the names of individuals is necessary to determine system use. [Redacted]

per Executive Secretary

DCI
EXEC
REG

CLASSIFIED BY SIGNER
DECLASSIFY OADR

L-108-IR NSDD
95

SECRET

CR: C-204-IR

25X1 SUBJECT: Proposed Secure Video Teleconferencing System
(SVTS) Concept of Operations [redacted]

25X1 DI/CPAS [redacted] (4 November 1988)

25X1

Distribution:

Orig - Addressee
1 - Executive Secretary
1 - Executive Registry
1 - DDI Registry
1 - DDI
1 - D/CPAS
1 - C/CPAS/Ops Ctr

MEMORANDUM FOR:

John

11/2/88

- Please add Office of Security to dissem on ER 88 4040X.
- Ops Center is preparing response, but I should have sent request to O/S also.

STAT

Done 03 NOV 1988

Date

FORM 107 USE PREVIOUS EDITIONS

★U

CONTROL NO. _____

CROSS REF: _____

PRIOR PAPERS ON THIS SUBJECT: NO YES

PRIOR CORRES SENT TO: _____

OTHER COMMENTS: _____

EXECUTIVE REGISTRY FILE NO: ~~SECRET~~

L-108-1R
NSDD 95

CROSS REF: _____

C-204-1R

EXECUTIVE SECRETARIAT**ROUTING SLIP**

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR				
4	D/ICS				
5	DDI	X			
6	DDA				
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OCA				
14	D/PAO				
15	D/PERS				
16	D/Ex Staff				
17	D/CPAS		X		
18	NIO/W		X (w/o att)		
19	Chmn/IHC		X (w/o att)		
20	D/OS		X ADDED 3 Nov 88		
21					
22	ER		X		
SUSPENSE		(noon) 7 Nov 88 Date			

Remarks To 5: Chief, Operations Center is preparing comments for transmittal by ES. (NIO/W and Chm/IHC also tasked for response--see NSC addressee list.)

STAT

ER 88-4040X

Executive Secretary

26 Nov 88

Oct Date

3637 (10-81)

SECRETNATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

ER 88-4040X

October 25, 1988

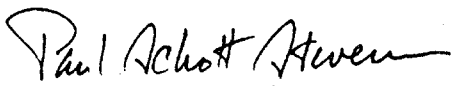
MEMORANDUM FOR DISTRIBUTION

SUBJECT: Proposed Secure Video Teleconferencing System
(SVTS) Concept of Operations (U)

A proposed Secure Video Teleconferencing System (SVTS) Concept of Operations is attached at Tab B for your review and concurrence. (U)

This document is the product of interagency discussions within the Crisis Management Working Group (CMWG) (current membership at Tab C). The focus and emphasis of the proposed concept of operations is the result of inputs from the CMWG's Operations Center Subgroup membership. (S)

We would appreciate your concurrence and comments on the attached draft by November 7, 1988. (U)


Paul Schott Stevens
Executive Secretary

Attachments

Tab A	List of Addressees
Tab B	Draft Secure Video Teleconferencing System (SVTS) Concept of Operations
Tab C	Current CMWG Membership

SECRET

Declassify on: OADR

SECRETC-108-15
NSDD 95

T
A
B

A



MR. DONALD GREGG
Assistant to the Vice President
for National Security Affairs

COL WILLIAM V. BOGART
Commander, White House
Communications Agency

MR. MELVYN LEVITSKY
Executive Secretary
Department of State

CAPT ANTHONY MANESS
Executive to the Chairman
Joint Chiefs of Staff

MS. JENNIFER A. SOUR
Executive Secretary
Department of Treasury

MR. JONATHAN F. THOMPSON
Executive Director
Office of Science and
Technology Policy

COL GEORGE P. COLE, JR.
Executive Secretary
Department of Defense

MR. JAMES GEER
Assistant Director of the
Intelligence Division
Federal Bureau of Investigation

MR. ROBIN ROSS
Chief of Staff
Department of Justice

MR. WILLIAM C. TIDBALL
Chief of Staff
Federal Emergency Management
Agency

STAT
MS. RUTH KNOUSE
Director,
Executive Secretariat
Department of Transportation

[Redacted]
Chief of Staff
National Security Agency

MS. DENISE A. HOWE
Manager, Administrative Staff
Federal Aviation Administration

COL CHARLES C. KRULAK
Deputy Director
White House Military Office

MR. WILLIAM V. VITALE
Executive Secretary
Department of Energy

LTG JOHN T. MEYERS
Manager
National Communications System

STAT
MR. L. WAYNE ARNY, III
Associate Director for
National Security and
International Affairs
Office of Management and Budget

[Redacted]
Deputy Director for JCS Support
Defense Intelligence Agency

STAT
[Redacted]
Executive Secretary
Central Intelligence Agency

[Redacted]
Chairman, Intelligence
Handling Committee
Intelligence Community Staff

COL E. R. CARWISE
Chief of Staff
Defense Communications Agency

COL KENNETH E. BAKER
Assistant Director for
Mobilization Plans
Defense Mobilization Systems
Planning Activity

COL RICHARD E. TREDINNICK
Program Manager, SVTS
Defense Communications Agency

MR. CHARLES E. ALLEN
National Intelligence Officer
for Warning
Central Intelligence Agency

T
A
B
B

SECRET

DRAFT

**SECURE VIDEO TELECONFERENCING
SYSTEM (SVTS)**

CONCEPT OF OPERATIONS (U)

October 20, 1988 Version

**Drafted by the
Crisis Management Working Group's
Operations Center Subgroup**

Classified by: NSC Staff
Declassify on: OADR

SECRET

SECURE VIDEO TELECONFERENCING SYSTEM (SVTS) CONCEPT OF OPERATIONS (U)

1. SVTS Mission Description. The purpose of the SVTS is to provide a secure video conferencing and information exchange system for government officials involved in the national security policy process. The system is primarily designed for use during international crises or domestic emergencies as a part of the National Security Information & Situation Management System (NSI&SMS). As such, the SVTS is one of a number of secure communications networks that exist within the operations/intelligence center community. When it is not being used by high-level officials, it may be made available to support other operational needs during a crisis, or for routine interagency conferencing/meetings. (S)

2. Capabilities. The SVTS shall support all levels of classified exchanges through TOP SECRET Sensitive Compartmented Information (SCI), to include special access programs. Each node shall provide the user a variety of secure, interactive media available for conferencing and information exchange. The system will support three simultaneous conferences with up to six nodes each. Specific capabilities shall include: (S)

- a. Near full-motion video with associated audio
- b. Full duplex audio conferencing capabilities
- c. Text processing and transfer
- d. Data transfer
- e. Freeze frame color graphics and annotations
- f. High resolution "gray scale" graphics
- g. Color and black and white printers

3. Policy Guidelines. (S)

a. References. (S)

- (1) NSDD-95, Crisis Information and Management System: PROJECT MEDUSA (S), May 1983 (superseded by NSDD 314)
- (2) NSDD-314, National Security Information & Situation Management System (TS), September 1988
- (3) NSDD-276, National Security Council Interagency Process (U), June 1987

SECRET

- 1 -

- (4) Network Security Manual (S), October 1987
 - (5) Draft SVTS Network Security Officer's Security Guide (S), May 1988
 - (6) Configuration Management Plan for SVTS
- b. Use of SVTS Within the NSC Process. The NSC policy process involves a hierarchy of formal policy deliberation groups, including the National Security Planning Group, Special Situation Group, Senior Review Group, and Policy Review Group. These groups review current national security situations (to include continuity of government issues), formulate options, recommend/decide upon courses of action, and track implementation of decisions. The SVTS is one of several vehicles for conducting these policy deliberations, especially in situations where time is critical and does not allow the physical assembly of the principals. It is also used as a vehicle for exchanging data amongst the various departments and agencies in support of the principals and the policy process. In this regard, it may be used by crisis information managers at various operations/intelligence centers to coordinate information production and support during crisis situations. It should also be available to support the larger day-to-day activities of the interagency policy process, such as meetings of interagency groups and interagency working groups that deliberate over ongoing situations, consider continuity of government activity, exchange indications and warning data and essential elements of information, and the like. (S)
- c. Priorities for Use. (S)
- (1) The National Security Council and statutory advisors (as defined in the National Security Act of 1947)
 - (2) Other cabinet-level officials
 - (3) Senior sub-Cabinet officials
 - (4) Directors of National-level intelligence agencies
 - (5) Duty personnel at operations and intelligence centers
 - (6) Interagency groups (e.g., SIGs, IGs)
 - (7) Organizations or activities with a primary operational or intelligence mission (e.g., interagency watch committee)

SECRET

- (8) Public affairs activities during national security crises or domestic emergencies
 - (9) Others (e.g., agency legislative affairs representatives) for use in conducting day-to-day activities
 - (10) The White House is assigned the only preemption capability
- d. Scheduling. Use of the SVTS shall be scheduled through the Hub Activity -- first come, first served, based upon the priorities listed above. The Hub shall: maintain a real time scheduling record; regularly publish and distribute a schedule, specifying "level" of prospective conferences, as well as unreserved time not being used for servicing; and maintain a log of department and agency contacts for purposes of resolving scheduling conflicts. To the maximum extent, preventive maintenance will be scheduled during other than normal duty hours. The SVTS Project Office is charged with the responsibility of investigating the potential for automated scheduling and display of system availability to the users. (S)
- e. Availability. The SVTS must be available to support national level decision makers on short notice. All SVTS nodes collocated with a 24-hour operations/intelligence center, must be able to establish a conference within 15 minutes following notification. Other nodes will provide a listing of 24-hour points of contact to be maintained by the Hub Activity. (S)
- f. Documenting System Use. Each node shall be responsible for maintaining a log of conferences initiated by that node. The log shall be classified at least SECRET, and should include date, time, classification and type (not subject) of conference (e.g. weekly intelligence watch committee, legislative affairs meeting, cabinet discussions, PRG), name of individual chairing the session, and names of participating agencies. This information will be provided via periodic reports, with the frequency designated by the Crisis Management Working Group (CMWG), to the SVTS Project Office for use in analyzing system usage. The SVTS Project Office will brief the Crisis Management Working Group (CMWG) at least semiannually on system usage and other related matters. To ensure privacy, details concerning individual conferences shall not be maintained by NISSOs. Responsibility for notetaking concerning the substance of a conference shall belong to the convening agency/office. (S)

SECRET

- 3 -

- g. Privacy. The system has been designed to accommodate information which is not only highly classified, but data that may be highly sensitive even though it is not classified. Senior officials that use the system must have reasonable assurance that there is no possibility of intrusion into their conversations with counterparts. Privacy is ensured through cryptographic, electronic, mechanical and acoustical isolation, and procedural and locational isolation methods. Recording of the video or audio portions of a conference is prohibited unless approved ahead of the event by the CMWG or its designated representative. (S)

4. Configuration Control. A configuration control program shall be instituted to ensure that any changes to the Government-approved system will support the continuing integrity and security of SVTS capabilities. Any changes to system nodes, such as physical movement of consoles, cameras, printers, etc., or introduction of new communications-electronics, use of external ports, and data processing or other equipment, must be approved prior to implementing any alterations. Accordingly, any changes to the SVTS shall be approved by the CMWG (the Configuration Control Board) through the use of approved procedures and processes specified in the SVTS Configuration Management Plan, as administered by the SVTS Project Office. The Configuration Control Board shall have sole authority to authorize waivers to integrity and security standards. The configuration Control board shall also review and approve all plans and concepts for operations for use of external ports. SVTS node managers must insure that any equipment tied to the system via external ports complies with integrity and security requirements. (C)

5. Security Requirements. Due to the senior government level use of the SVTS and the information carried on it, it would be a prime target for hostile intelligence forces if the specifics of its existence (node configuration and system design) and operation were disclosed. Accordingly, any listing of the SVTS nodes or description of node capabilities and system description shall be classified SECRET. On the other hand, the terms SVTS and secure video teleconferencing are UNCLASSIFIED. Access to individual nodes, or the disclosure of a particular node's existence, may be provided to properly cleared individuals with valid need-to-know, without a requirement for special documentation. Personnel security access procedures will be in accordance with existing law and directives, and the SVTS Network Security Manual. (S)

- a. The SVTS Network Security Manual shall stipulate basic security policy, requirements, and procedures to operate and maintain the SVTS network. It shall also include a security classification guide. (C)

SECRET

- b. As presently configured, the SVTS is a telecommunications tool rather than a computer system that stores classified information. It shall, to the maximum possible extent, be governed by telecommunications security guidelines. System security features (e.g., log-on/passcode procedures and security alarms) shall be instituted in such a manner as to maximize user convenience and operational effectiveness while remaining consistent with security requirements of the system. [REDACTED] shall be required for each node. In addition, security

25X1

25X1

[REDACTED]
that a scheduled conference not be activated or that any ongoing conference be discontinued. (S)

- c. The SVTS Network Security Officer's Security Guide shall identify specific security procedures necessary to ensure the efficient and secure operation of the SVTS. This guide will include such information as access requirements, information security guidelines, and standard operating procedures. (C)

6. Responsibilities: (S)

- a. NSC. The NSC chairs the interagency Crisis Management Working Group (CMWG) that provides policy guidance concerning all aspects of the SVTS and deals with oversight and policy coordination of the larger National Security Information & Situation Management System (NSI&SMS). (S)

- b. DoD. The Department of Defense is assigned responsibility as Executive Agent for the NSI&SMS, which includes SVTS development, installation, training, logistical support, configuration management, system security/accreditation, and architectural/engineering support to system modernization. In addition, the Department shall (1) act as the Designated Approving Authority (DAA), responsible for providing approval for the operation of SVTS; and (2) designate a Network Security Officer who has the overall responsibility for monitoring all SVTS network security matters. (S)

- c. [REDACTED] the Hub Information System Security Officer (HISSO). WHCA is also responsible for scheduling use and maintenance of the system, for maintaining listings of authorized users and after-hours points of contact, and for documenting and reporting on system usage. (S)

25X1

- d. NSO. The Network Security Officer (NSO), designated by

SECRET

- 5 -

the the DoD, will be responsible for: monitoring all security aspects of the network; certifying all SVTS nodes; and providing guidance to the Hub Information System Security Officers (HISSOs) and Node Information System Security Officers (NISSOs) in implementing security guidance approved by the CMWG. The NSO shall chair the Network Certification Working Group (NCWG). (S)

- e. DCA. The Defense Communications Agency shall function as the SVTS Program Office, fulfilling those responsibilities delegated by DoD as the program Executive Agent. These include architectural and engineering support, following initial SVTS installation and acceptance, and configuration management. (S)
- f. Nodes. Each using department or agency shall be responsible for operating their system and for ensuring their respective nodes are capable of supporting national-level decision makers during national security crises and domestic emergencies in accordance with established procedures and security guidelines. The NISSOs are responsible for physical and administrative security of their respective nodes, and for establishing procedures which will ensure proper security clearance and access of those individuals participating in SVTS conferences. Those charged with staffing the SVTS must be properly trained and provided with adequate local operating procedures to effectively support operations. Each participating department or agency shall fund maintenance, training and CMWG approved modernization to SVTS equipment or facilities. In addition, each node shall be responsible for the accreditation of their facility. (S)

SECRET

- 6 -

APPENDIX I

DEFINITION OF TERMS (U)

1. Crisis Management Working Group: An interagency group responsible for further development of the National Security Information & Situation Management System (NSI&SMS) and for strengthening interagency capabilities and procedures for the collection, coordination, transmission, and dissemination of information in support of the President and the National Security Council (NSC) interagency process. (C)
 2. Critical Failure: Any failure of the SVTS that makes it unable to perform its required function. (C)
 3. DAA: The Designated Approving Authority is the accreditor for the SVTS network. The Department of Defense is the DAA. (U)
 4. External Ports: Electronic connections that provide the capability to integrate external video, audio, data, graphics, and other sources with the SVTS. (S)
 5. Freeze Frame Graphics: The transmission or reception and real-time annotation of single-frame, low resolution graphic images such as line drawings, maps, and charts. (S)
 6. High Resolution Graphics: The transmission or reception of high quality graphics material such as single frame, detailed maps, imagery, photographs, and hardcopy text. (S)
 7. HISSO: The Hub Information System Security Officer responsible for the secure operations of the Hub facility including system maintenance and control. The White House Communications Agency (WHCA) is the HISSO. (C)
-
9. Manual Capability: System networking achieved by manual patching of the nodes at the Hub and the electro-mechanical operation of SVTS controls by the operators, as opposed to the automated system which is connected by dedicated computer software at the Hub and touch-screen controls for operators. (C)
 10. Multi-line voice telephone: A communications device capable of secure, dial-up, telephone quality voice transmission

25X1

SECRET

- 7 -

or reception. (S)

11. National Security Information & Situation Management System (NSI&SMS): An interagency network of people, facilities, equipment, information resources, plans, policies and procedures designed to provide for (1) support to national-level decision makers in monitoring national security situations and in considering, implementing, or reporting on any U.S. response; and (2) a rapid and continuous flow of information regarding national security situations across a spectrum from peacetime activity through reconstitution following nuclear attack. The system also supports, to the maximum possible extent, the interagency process applying to domestic emergencies, such as natural disasters, terrorism, or technological hazards that may affect US national security interests. (S)

12. Network Certification Working Group: An interagency group chaired by the Network Security Officer (NSO) that is responsible for security matters of the SVTS network. (U)

13. NSO: The Network Security Officer is appointed by the DAA and manages the implementation of the security requirements of the system. The National Security Agency is the NSO. (U)

14. NISSO: The Node Information System Security Officer responsible for the overall secure operations of the user node facility at his/her site, including cryptographic security and physical security. (U)

15. Node: All of the SVTS telecommunications and support facilities and equipment located at a user site. (U)

16. Privacy: The reasonable assurance that the information being transmitted in the SVTS is not accessible to other than intended recipients. (S)

17. Reliability: A measure of the SVTS capability to provide responsive and dependable system performance. (U)

18. Reliability Standards: Node and Hub reliability should allow for 30-days minimum time between preventive maintenance, and 30 days mean time between critical failures. (These standards shall be clarified in a forthcoming DCA review.) (S)

19. SVTS Executive Agent: The Department of Defense. (U)

20. SVTS Project Office: The Defense Communications Agency, responsible for program design, development and implementation for the SVTS. (U)

21. Video Teleconferencing: The simultaneous transmission of one and reception of five near full-motion video images and associated audio. (U)

SECRET

- 8 -

22. WHCA: The White House Communications Agency. (U)

23. Word Processing: The transmission or reception of word processed textual material and real-time transmission or reception of text editing. (U)

SECRET

- 9 -

[REDACTED]

T
A
B

C

CURRENT CMWG MEMBERSHIP:

OFFICE OF THE VICE PRESIDENT: Samuel Watson
Deputy Assistant to the VP (for National Security Affairs)

WHITE HOUSE MILITARY OFFICE: Colonel Charles C. Krulak,
Deputy Director

DEPARTMENT OF STATE: Joseph E. Lake
Director, Operations Center

DEPARTMENT OF TREASURY: Randall Fort,
Special Assistant to the Secretary (National Security)

DEPARTMENT OF DEFENSE: Shirl Axtell
Director, OSD Crisis Coordination Center

DEFENSE INTELLIGENCE AGENCY:
Chief, NMIC Operations Support Branch, JSO

25X1

DEFENSE COMMUNICATIONS AGENCY: David T. Signori
Director, Center for Command & Control and Communications
Systems

DEPARTMENT OF JUSTICE: D. Jerry Rubino
Director of Emergency Security Planning
Justice Management Division

FEDERAL AVIATION ADMINISTRATION: Jerome Cohen
Manager, Emergency Operations Staff

DEPARTMENT OF ENERGY: Captain Jay G. McDonald
Director of Emergency Operations, O/ASD (Programs)

OFFICE OF MANAGEMENT AND BUDGET: Arnold E. Donahue
Chief, Intelligence Branch, National Security Division, NS/IA

CENTRAL INTELLIGENCE AGENCY:
Director, Operations Center

25X1

CENTRAL INTELLIGENCE AGENCY: Charles E. Allen, National
Intelligence Officer for Warning

ORGANIZATION OF THE JOINT CHIEFS OF STAFF: LTC Raymond W.
O'Keefe, Chief, Operations Training Branch

OFFICE OF SCIENCE AND TECHNOLOGY POLICY: John O'Neil, Senior
Policy Analyst, Directorate for National Security Affairs

FEDERAL BUREAU OF INVESTIGATION: Joseph Cantamessa, Jr.
Supervisory Special Agent, Criminal Investigative Division

SECRET

FEDERAL EMERGENCY MANAGEMENT AGENCY: Keith R. Peterson,
Chief, Readiness Division

STAT

INTELLIGENCE COMMUNITY STAFF: [REDACTED]
Chairman, Information Handling Committee

25X1

STAT

NATIONAL SECURITY AGENCY: [REDACTED]
Chief, Special Projects Staff (P-303)

25X1

DEFENSE MOBILIZATION SYSTEMS PLANNING ACTIVITY: Colonel Kenneth
E. Baker, Assistant Director for Mobilization Plans

NATIONAL COMMUNICATIONS SYSTEM: Colonel Robert C. Sparks
Assistant Manager for Emergency Preparedness

SECRET